복합위협에 대한 대응방안 동적 조합 프레임워크

송유래[1], 김득훈[2], 곽진[3]
[1]아주대학교 사이버보안학과 정보보호응용및보증연구실 석사과정
[2]아주대학교 소프트웨어융합연구소 박사후연구원
[3]아주대학교 사이버보안학과 교수
clara701@ajou.ac.kr, dhkim.isaa@gmail.com, security@ajou.ac.kr

Countermeasure Dynamic Combination Framework against Blended Threat

Yu-Rae Song[1], Deuk-Hun Kim[2], Jin Kwak[3]
[1]ISAA Lab., Dept. of Cyber Security, Ajou University
[2]Inst. for Computing and Informatics Research, Ajou University
[3]Dept. of Cyber Security, Ajou University

요 약

IoT(Internet of Things) 기기를 활용하는 분야가 증가함에 따라 스마트 팩토리, 스마트 그리드 등 융합환경이 발전되었으며, 융합환경이 상호연결되는 IoBE(Internet of Things Blended Environment)가 조성되고 있다. 그러나, IoBE 구성요소가 복잡해짐에 따라 공격 표면이 증가하고, 기존에 알려진 보안위협이 융·복합되어 새로운 형태의 보안위협인 복합위협(BT, Blended Threat)이 발생할 수 있다. BT는 다양한 보안위협이 복합적으로 연계되어 발생함에 따라 예측하여 대응하기에 기존 보안위협보다 상대적으로 어려우며, 이에 대응방안 간의 조합을 통해 보안위협에 유동적으로 대응하는 동적 보안 프레임워크가 필요하다. 따라서, 본 논문에서는 BT에 대한 대응방안 동적 조합 프레임워크를 제안한다.

1. 서론

산업계, 의료계 등 다양한 분야에서 IoT(Internet of Things) 디바이스를 활용하게 되며 스마트 팩토리, 스마트 그리드 등의 융합환경이 조성되고, 융합환경들이 상호연결되며 IoBE(Internet of Things Blended Environment)로 발전하고 있다. 이에 따라 IoBE 구성요소 간의 연결이 복잡해져 공격 표면이 증가하고 있으며, 증가한 공격 표면에서 보안위협이 융·복합된 복합위협(BT, Blended Threat)이 발생할 수 있다. BT는 다양한 보안위협이 복합적으로 연계되어 발생하므로 기존 보안위협보다 예측하기 어렵다. 이에 따라, 대응방안의 조합을 통해 보안위협에 유동적으로 대응하는 보안 프레임워크가 필요하다. 따라서, 본 논문에서는 예측의 어려움에 대응하기 위해 대응방안을 보안위협과 매칭시켜 동적으로 조합하는 보안 프레임워크를 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 IoBE, BT의 정의와 IoBE 구성요소 간 관계를 설명하고, 3장에서는 IoBE 구성환경의 공격 표면별 보안위협 대응방안을 분석한다. 그리고 4장에서 대응방안 동적 조합 프레임워크를 제안한 뒤 5장에서 결론을 맺는다.

2. 관련연구

2.1 IoBE

IoBE는 스마트 팩토리, 스마트 그리드 등과 같은 융합환경이 상호연결된 환경으로, 융합환경은 센싱, 네트워킹, AI(Artificial Intelligence), 클라우드 등의 IT 기술이 융합되어 IoT 디바이스들이 복잡하게 연결된 환경을 의미한다. 이때, IoBE 내 상호연결되는 환경이 증가할수록 IoBE 내에 포함된 IoT 디바이스 간 연결이 복잡해지며, 증가한 공격 표면 대상 공격에 대한 대응 연구가 진행 중이다. IoBE를 구성하는 융합환경 내 공격 표면 예시는 <표 1>과 같다[1].

<표 1> IoBE 내 융합환경의 공격 표면 예시

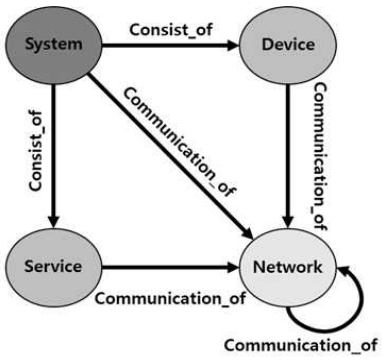
Environment	Attack Surface
Smart Factory	Physical access, Industrial control system, Factory control network, Factory work domain, Supply chain, Personnel and aging equipment, etc.
Digital Healthcare	Medical devices, Medical info system, Digital healthcare network, etc.

Environment	Attack Surface
Smart Grid	AMI(Advanced Metering Infrastructure), ESS(Energy Storage System), EV(Electric Vehicle) charging system, EMS(Energy Management System), etc.
Smart Building	CCTV system, Access control system, HVAC(Heating, Ventilating and Air Conditioning), Fire alarm systems, IBMS(i-Building Management System) etc.
C-ITS (Cooperative-Intelligent Transport System)	Physical access, Supply chain, Traffic control system, V2X(Vehicle to Everything) communication, etc.

2.2 BT

BT는 IoBE 내 융합환경을 구성하는 플랫폼, 디바이스 아키텍처, 네트워크 프로토콜 등의 취약점을 통해 발생 가능한 복합위협이다. IoBE 내 구성요소가 많아질수록 다양한 보안위협이 복합적으로 연계되어 발생 가능한 보안위협 예측에 어려움이 존재하며, 이에 대응하기 위해 BT 대응 관련 연구가 수행되고 있다[1, 2].

2.3 IoBE 구성요소 간 관계



(그림 1) IoBE 구성요소 관계도

IoBE 구성요소 간 관계도는 (그림 1)과 같으며, 구성요소 간의 관계를 정형적으로 기술하는 도메인 온톨로지를 활용하여 정의된다. System, Device, Service, Network 4가지로 구성되며, System은 Device와 Service를 구성요소로 포함하고(Constist_of), System, Device, Service, Network는 Network를 통해 상호연결된 것(Communication_of)을 확인할 수 있다[2].

3. IoBE 내 공격 표면별 보안위협 대응방안 분석

IoBE 내 공격 표면을 대상으로 하는 보안위협에 대해 대응방안을 <표 2>와 같이 도출하였다. 이를 통해 보안사고 발생 시 보안위협별로 적절한 대응방안을 매칭하여 적용할 수 있다.

<표 2> 공격 표면별 보안위협 대응방안 예시

Environment	Attack Surface	Countermeasure
Smart Factory	Physical access	Physical AC(Access Control)/Separation, etc.
	Industrial control system	Encryption, IDS, etc.
	Factory control network	DLP(Data Loss Prevention), Firewall, etc.
	Factory work domain	Network Separation, Encryption, etc.
	Supply chain	Status Monitoring, Network Separation, etc.
	Personnel and aging equipment	DLP, IDS, etc.
Digital Healthcare	Medical devices	Physical AC, Secure coding, etc.
	Medical info system	DLP, AC, etc.
	Digital healthcare network	Firewall, Encryption, etc.
Smart Grid	AMI	Encryption, IDS, etc.
	ESS	Encryption, Firewall, etc.
	EV charging system	Encryption, Integrity Verification, etc.
	EMS	DLP, IDS, etc.
Smart Building	CCTV system	Physical AC, IDS, etc.
	Access control system	Status Monitoring, RFID Security Technology, etc.
	HVAC	Integrity Verification, Encryption, etc.
	Fire alarm system	Physical AC, Status Monitoring, etc.
	IBMS	IDS, Integrity Verification, etc.

Environment	Attack Surface	Countermeasure
C-ITS	Physical access	Physical AC/ Separation, etc.
	Supply chain	Status Monitoring, Encryption, etc.
	Traffic control system	Encryption, IDS, etc.
	V2X com.	Status Monitoring, AC, etc.

4. 제안사항

대응방안 동적 조합 프레임워크는 Infrastructure 내 공격 표면에서 발생 가능한 BT에 대하여 CM(Collaborative Measure)을 도출한다. 이때 CM은 BT에 악용된 보안위협 각각에 매칭되는 대응방안이 동적으로 조합된 것이며, 대응방안 동적 조합 프레임워크의 단계를 (그림 2)와 같이 설명한다.

Step 1. 공격 표면에서 발생한 BT 분석

Infrastructure 내 공격 표면에서 발생한 BT를 분석하는 단계로, 어떠한 보안위협이 융·복합되어 BT를 구성하는지 분석한다.

Step 2. 각 보안위협에 대한 대응방안 매칭

BT를 구성하는 보안위협 각각에 대해 유동적으로 대응방안을 매칭하는 단계로, Step 1.에서 분석된 보안위협의 대응방안을 도출한다.

Step 3. BT에 대한 CM 도출

Step 2.에서 도출한 대응방안을 동적으로 조합하여 CM을 도출하는 단계로, BT의 진행에 따라 CM이 구성하는 대응방안을 단계별로 활용하여 BT에 대응한다.

예를 들어, 스마트 그리드 내 프로토콜(System) 취약점을 통해 HAN(Network) 서버에 침투하고 스마트 팩토리의 FEMS(Service) 에너지 사용량 변조를 수행한 뒤, 스마트 팩토리 프로토콜 취약점(System)을 통한 데이터 유출을 수행하는 BT가 발생하였을 때, 서버 침투, 원격 조정, 데이터 변조, 데이터 유출이 발생하는 지점에서 대응방안 동적 조합 프레임워크는 각각 접근 제어, 원격 접속 IP 차단, 데이터 위·변조 방지, DLP 등의 대응방안을 수행함으로써 공격에 대응할 수 있다.

5. 결론

본 논문에서는 IoBE 내 공격 표면을 대상으로 하는 BT에 대한 대응방안 동적 조합 프레임워크를 제안한다. 이를 통해 BT가 발생하였을 때 각 보안위협에 대응방안을 매핑하고 적절한 보안기술을 조합하여 적용 및 대응할 수 있을 것이다. 추후 공격 시나리오를 생성하여 제안한 동적 조합 프레임워크를 기반으로 실증을 수행할 예정이다.

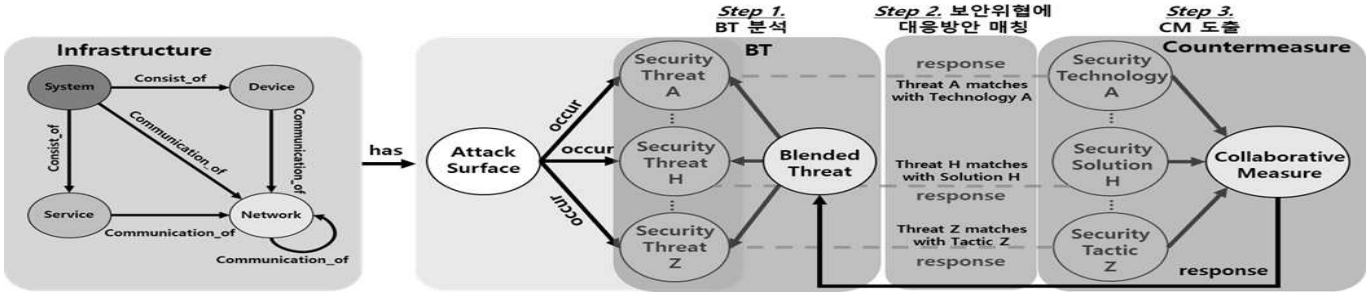
사사문구

이 논문은 2022년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(No. 2022R1I1A1A01073760) 및 2023년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2021R1A2C2011391).

참고문헌

[1] Minkyung Lee, Julian Jang-Jaccard, and Jin Kwak, “Novel Architecture of Security Orchestration, Automation and Response in Internet of Blended Environment”, CMC-Computers, Materials & Continua, Tech Science Press, Vol. 16, No. 7, pp. 119-223, Jul. 2022.

[2] Minkyung Lee, In-su Jeong., Deuk-Hun Kim, Julian Jang-Jaccard, and Jin Kwak, “Applicability Analysis of Knowledge Graph Embedding on Blended Threat”, 2022 International Conference on Platform Technology and Service(PlatCon), Jeju, Korea, 2022, pp. 48-52.



(그림 2) 대응방안 동적 조합 프레임워크